• **Classfield Theory** In brief, *global* classfield theory classifies *abelian* extensions of *number fields*, while *local* classfield theory does the analogous things for *local fields*, finite extensions of $\mathbb{Q}_p$.

The details subsume all known (abelian) **reciprocity laws**.

Approaching classfield theory:
- Rough classical statement of *global* classfield theory
- Statement of *local* classfield theory
- Recollection of facts about extensions of *finite* fields
- Unramified extensions of *local* fields
- Special case: unramified local classfield theory
- Special case: quadratic local classfield theory over $\mathbb{Q}_p$
- Kummer theory
- ...

Main Theorem of Global Classfield Theory (classical form): The abelian (Galois) extensions K of a number field k are in bijection with generalized ideal class groups, which are quotients of *ray class groups* of *conductor* (a non-zero ideal) $\mathfrak{f}$

$$I(\mathfrak{f})/P_{\mathfrak{f}}^{+}$$

$$||$$

$$\frac{\text{fractional ideals prime to } \mathfrak{f}}{\text{principal ideals with totally positive generators } 1 \bmod \mathfrak{f}}$$

Further, the bijection sends a given generalized ideal class group to the (abelian) *Galois group* of the extension, via the *Artin/Frobenius* map/symbols $\mathfrak{p} \to (\mathfrak{p}, K/k)$, characterized by

$$(\mathfrak{p}, K/k)(x) \;=\; x^q \mod \mathfrak{P} \qquad (x \in K,\ \mathfrak{P} \text{ over } \mathfrak{p},\ q = \#\mathfrak{o}_k/\mathfrak{p})$$

Main Theorem of Local Classfield Theory: The abelian (Galois) extensions K of a local field k are in bijection with the open, finite-index subgroups of $k^\times$, by

$$K/k \longleftrightarrow k^\times / N_k^K(K^\times)$$

This bijection is given by an isomorphism of the Galois group with $k^\times / N_k^K K^\times$ via Artin/Frobenius.

Cyclic local-global principle for norms: In a *cyclic* extension K/k of number fields, an element of k is a *global norm* if and only if it is a *local norm everywhere.* That is, for $\alpha \in k$,

$$\alpha \in N_k^K(K^\times) \iff \alpha \in N_{k_v}^{K_w}(K_w^\times) \text{ for all } v, w$$

Proof by analytic properties of *zeta functions of simple algebras.*

Finite fields: Recall the classification of finite algebraic field extensions of $\mathbb{F}_q$ with q a power of a prime p.

Unique extension of given degree: inside a fixed algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, there is a unique field extension K of given degree n over $\mathbb{F}_q$. This extension is the collection of roots of $x^{q^n} - x = 0$ in the fixed algebraic closure.

Galois group of $\mathbb{F}_{q^n}/\mathbb{F}_q$: is *cyclic*, generated by the Frobenius element $\alpha \to \alpha^q$.

Surjectivity of norms on finite fields: The Galois norm $N : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is *surjective:*

Surjectivity of traces on finite fields: The Galois trace $\mathrm{tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ is *surjective:*

Linear independence of characters: Distinct field maps $\chi_j : k \to \Omega$ are linearly independent: $\sum_j c_j \chi_j = 0$ for $c_j \in \Omega$, as a map $k \to \Omega$, only for c_j all 0.

Unramified extensions of $\mathbb{Q}_p$: Inside a fixed algebraic closure of $\mathbb{Q}_p$, for each positive integer n there is a unique *unramified* extension K of $\mathbb{Q}_p$ of degree n over $\mathbb{Q}_p$. It is generated by a primitive $p^n - 1$ root of unity.

Proof: Recall that the local ramification degree e and residue class field extension degree f satisfy $ef = n$. The unramified-ness is $e = 1$, so $f = n$. There is a primitive $p^n - 1$ root of unity in $\mathbb{F}_{p^n}$.

The $(p^n - 1)^{th}$ cyclotomic polynomial Φ has no repeated roots mod p, since $x^{p^n-1} - 1$ has none. Let $\zeta_1 \in \mathfrak{o}_K$ reduce to a primitive $p^n - 1$ root mod p, so $\Phi(\zeta_1) = 0 \bmod p$ and $\Phi'(\zeta_1) \neq 0 \bmod p$. Hensel produces a primitive $(p^n - 1)^{th}$ root of unity ζ in K, and $K = \mathbb{Q}_p(\zeta)$. All $(p^n - 1)^{th}$ roots of unity are powers of a given one, proving uniqueness of K. ///

Remark: The $(p^n - 1)^{th}$ cyclotomic polynomial Φ is *not* irreducible over $\mathbb{Q}_p$, since any root of $\Phi(x) = 0$ generates a degree n extension of $\mathbb{Q}_p$! It is a product of $\varphi(p^n - 1)/n$ irreducibles each of degree n, where φ is Euler's φ-function.

Remark: The same proof works over an arbitrary local field k with residue field having q elements: the unique unramified extension of degree n over k is obtained by adjoining a primitive $(q^n - 1)^{th}$ root of unity to k.

Therefore, the $(q^n - 1)^{th}$ cyclotomic polynomial Φ factors into $\varphi(q^n - 1)/n$ irreducibles of degree n over k.

Artin/Frobenius elements in Galois groups over $\mathbb{Q}_p$

In any finite extension $K/\mathbb{Q}_p$, there is certainly a unique prime $\mathfrak{p}$ over p. Thus, the *decomposition group* $G_\mathfrak{p} = \{g \in \mathrm{Gal}(K/\mathbb{Q}_p) : g\mathfrak{p} = \mathfrak{p}\}$ is the whole Galois group $\mathrm{Gal}(K/\mathbb{Q}_p)$.

Decomposition groups always *surject* to the residue field Galois groups. For unramified $K/\mathbb{Q}_p$, the latter is cyclic order n, generated by Frobenius. Since $[K : \mathbb{Q}_p] = n$, this surjection is an *isomorphism*.

Thus, $\mathrm{Gal}(K/\mathbb{Q}_p) = G_\mathfrak{p}$ is cyclic order n, with canonical generator denoted $(p, K/\mathbb{Q}_p)$ called the *Artin* symbol, a special case of *Frobenius*, characterized by reducing mod p to the finite-field Frobenius.

Remark: The same discussion applies to unramified extensions of arbitrary local fields: an unramified extension K/k of a local field k has cyclic Galois group with canonical generator the Artin/Frobenius $(\mathfrak{p}, K/k)$, where $\mathfrak{p}$ is the prime in $\mathfrak{o}_k$, characterized by

$$(\mathfrak{p}, K/k)(x) \;=\; x^q \mod \mathfrak{p}\mathfrak{o}_K \qquad\qquad (x \in \mathfrak{o}_K, \text{ where } q = \#\mathfrak{o}_k/\mathfrak{p})$$

In situations like this where there is a single prime lying over $\mathfrak{p}$

Claim: The Galois norm $N : K \to k$ of local fields gives a *surjection* on local units $\mathfrak{o}_K^\times \to \mathfrak{o}_k^\times$.

[Proof was by surjectivity of norms on *finite* fields, as well as surjectivity of *traces*, and completeness of k.]

A very special sub-case: *unramified* **local classfield theory:**

(Mock) Theorem: Unramified extensions K of a local field k are in bijection with finite-index subgroups of $k^\times$ containing $\mathfrak{o}_k^\times$, by

$$\text{finite-index subgroup } H \supset \mathfrak{o}_k^\times \quad \longleftrightarrow \quad N_k^K(K^\times)$$

The Galois group is $\mathrm{Gal}(K/k) \approx k^\times/N_k^K(K^\times)$, via the map to Artin/Frobenius:

$$\mathfrak{p} \quad \longrightarrow \quad (\mathfrak{p}, K/k) \qquad\qquad (\text{giving } x \to x^q \bmod \mathfrak{p}\mathfrak{o}_K)$$

Proof: We have shown that an unramified extension K of k of degree n is cyclic Galois, obtained by adjoining a primitive $(q^n - 1)^{th}$ root of unity ω, and the map from $\mathrm{Gal}(K/k)$ to the Galois group of residue fields is an isomorphism. Thus, the Artin/Frobenius $(\mathfrak{p}, K/k)$ generates $\mathrm{Gal}(K/k)$, and is order n.

Since the norm $N_k^K : \mathfrak{o}_K^\times \to \mathfrak{o}_k^\times$ is surjective, the image $N_k^K(K^\times)$ contains the open subgroup $\mathfrak{o}_k^\times$ of $k^\times$, so is *open*. Since K/k is unramified, a local parameter ϖ in k remains a local parameter in K, and $N_k^K(\varpi) = \varpi^n$. Thus,

$$k^\times / N_k^K(K^\times) \approx \varpi^{\mathbb{Z}} / \varpi^{n\mathbb{Z}}$$

which gives the Galois group, by the map $\varpi^\ell \to (\mathfrak{p}, K/k)^\ell$.

On the other hand, for $H \supset \mathfrak{o}_k^\times$ of finite index n, since $k^\times/\mathfrak{o}_k^\times \approx \varpi^{\mathbb{Z}}$, necessarily $H = \varpi^{n\mathbb{Z}} \cdot \mathfrak{o}_k^\times$. Adjoining a primitive $(q^n - 1)^{th}$ root of unity produces an unramified degree n extension K such that $N_k^K(K^\times) = H$. ///

Remark: This reformulation of the classification of unramified extensions of local fields is not terribly useful, but illustrates the type of formulation *necessary* for more general abelian extensions, in local classfield theory.

Another special sub-case: **quadratic extensions of $\mathbb{Q}_p$, $p \neq 2$:**

(Mock) Theorem: Let $p > 2$. The quadratic extensions K of $\mathbb{Q}_p$ are in bijection with the subgroups H of index 2 in $\mathbb{Q}_p^\times$, by

$$K \longleftrightarrow \mathbb{Q}_p^\times / N_{\mathbb{Q}_p}^K(K^\times)$$

The extension $K/\mathbb{Q}_p$ is unramified if and only if $N_{\mathbb{Q}_p}^K(K^\times) \supset \mathbb{Z}_p^\times$.

Remark: Since every field contains ± 1, and ± 1 are *distinct* in characteristic not 2, the theory of quadratic extensions is a special case of *Kummer theory*, which more generally discusses cyclic extensions of order n over ground fields of characteristic not dividing n and containing n^{th} roots of unity.

Proof: The unramified quadratic case is included in the general discussion of unramified extensions, of course. But the immediate issue is to understand the Kummer-theory quotient $k^\times/(k^\times)^2$.

Recall that the exponential map $x \to e^x = \sum_{n=0}^\infty \frac{x^n}{n!}$ converges p-adically for $\mathrm{ord}_p x > \frac{1}{p-1}$, since

$$\mathrm{ord}_p\, n! \;<\; \frac{n}{p} + \frac{n}{p^2} + \ldots \;=\; \frac{n/p}{1-\frac{1}{p}} \;=\; n \cdot \frac{1}{p-1}$$

This also applies to ord_p and/or $|\cdot|_p$ *extended* to field extensions K of $\mathbb{Q}_p$. Not *composed* with Galois norm, but, rather, *extended*. Similarly, $-\log(1-x) = \sum_{n\ge 1} \frac{x^n}{n}$ converges for $\mathrm{ord}_p x > 0$, since

$$\mathrm{ord}_p\, n \;\le\; \log_p\, n \;\ll_\varepsilon\; n^\varepsilon \qquad\qquad (\text{for all } \varepsilon > 0)$$

The immediate point of considering these functions is to give the isomorphism of the subgroup of units $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ to $p\mathbb{Z}_p$. In particular, *everything* in $1+p\mathbb{Z}_p$ is a *square* for $p > 2$, since $2 \in \mathbb{Z}_p^\times$.

(This, or some equivalent, is the most technical part of this discussion.)

Next, to understand squares in $\mathbb{Z}_p^\times$, consider

$$1 \longrightarrow 1 + p\mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times \longrightarrow (\mathbb{Z}/p)^\times \longrightarrow 1$$

Since everything in $1 + p\mathbb{Z}_p$ is a square, an element of $\mathbb{Z}_p^\times$ is a square if and only if its image in $(\mathbb{Z}/p)^\times$ is a square. The latter group is cyclic of order $p-1$, so the squares are of index 2.

To understand squares in $\mathbb{Q}_p^\times$, choice of the usual local parameter p gives a splitting $\mathbb{Q}_p^\times \approx \mathbb{Z}_p^\times \times p^{\mathbb{Z}}$, and

$$\begin{array}{ccccccccc} 1 & \to & (\mathbb{Z}_p^\times)^2 \times (p^2)^{\mathbb{Z}} & \to & \mathbb{Z}_p^\times \times p^{\mathbb{Z}} & \to & \{1,\varepsilon\} \times \{1,p\} & \to & 1 \\ & & || & & || & & & & \\ & & (\mathbb{Q}_p^\times)^2 & & \mathbb{Q}_p^\times & & & & \end{array}$$

where ε is a non-square unit (modulo squares of units). Thus, $\mathbb{Q}_p^\times$ modulo squares is a $2,2$ group, with representatives $1, \varepsilon, p, \varepsilon p$. Since $\mathbb{Q}_p(\sqrt{p})$ and $\mathbb{Q}_p(\sqrt{\varepsilon p})$ are visibly ramified: the square root is a uniformizer in the extension, and has $\mathrm{ord}_p = \frac{1}{2}$. Equally visibly, $\mathbb{Q}_p(\sqrt{\varepsilon})$ is the unique unramified quadratic extension. (This all uses $p > 2$!)

To make this a special case of local classfield theory, examine the norms from each of the three quadratic extensions for $p > 2$.

In the unramified extension, local units are norms, and the norm of $p^{\mathbb{Z}}$ hits $p^{2\mathbb{Z}}$, so the norm index is 2, and p is not a norm.

For the ramified quadratic extensions K, the norm is

$$N(a + b\sqrt{\varepsilon p}) \;=\; a^2 - \varepsilon p b^2$$

Certainly $-\varepsilon p$ is a norm, and is a local parameter, so $\mathbb{Q}_p^\times / N(K^\times)$ has representatives among *units.* From the norm expression, unit norms are squares mod p. Thus, the index is *at least* 2.

Thus, it suffices to show that $1 + p\mathbb{Z}_p$ is hit by norms. Since $N(1 + px) = (1 + px)^2$ for $x \in \mathbb{Q}_p$, and $1 + p\mathbb{Z}_p$ consists entirely of squares for $p \;>\; 2$, the index inside the units is *exactly* 2 for ramified quadratic extensions. ///

General Kummer theory: Recall that cyclic extensions K of degree dividing n of a field k of characteristic not dividing n and containing n^{th} roots of unity are in bijection with cyclic subgroups of $k^\times/(k^\times)^n$, by $K = k(\sqrt[n]{\alpha}) \longleftrightarrow \langle\alpha\rangle \bmod (k^\times)^n$.

Proof: On one hand, certainly $k(\sqrt[n]{\alpha}) = k(\sqrt[n]{\alpha\beta^n})$.

On another hand, let G be the Galois group of cyclic K over k. Since k contains n^{th} roots of unity, the commuting k-linear endomorphisms of K given by G are *simultaneously diagonalizable.* Since this assertion is central to this proof of the theorem of Kummer theory, we give details.

To get an idea how to proceed, observe that the minimal polynomial $P(x) = \prod_\zeta (x-\zeta)$ of a generator g of G has roots n^{th} roots of unity. For each root ζ, with $Q_\zeta(x) = P(x)/(x-\zeta)$, $Q_\zeta(g)$ is not the 0 endomorphism of K, so there is $\alpha \in K$ such that $Q_\zeta(g)(\alpha) \neq 0$. Nevertheless, $(g-\zeta)Q_\zeta(g)(\alpha) = P(g)(\alpha) = 0$. Thus, $Q_\zeta(g)(\alpha)$ is a (non-zero) ζ-eigenvector for g.

Since $g^n = 1$, the minimal polynomial of g divides $x^n - 1$, which has no repeated roots when the characteristic does not divide n. Thus, g is *diagonalizable*, meaning that K is the direct sum of g's eigenspaces. Indeed, as ζ runs over roots of $P(x) = 0$, the quotients $Q_\zeta(x) = P(x)/(x - \zeta)$ have collective common factor 1. Thus, there are monic $R_\zeta(x) \in k[x]$ such that

$$1 \;=\; \sum_\zeta R_\zeta(x) \cdot Q_\zeta(x) \qquad \text{and} \qquad 1 \;=\; \sum_\zeta R_\zeta(g) \cdot Q_\zeta(g)$$

Thus, $K = \bigoplus_\zeta \Big(R_\zeta(g) \cdot Q_\zeta(g)\Big)(K)$ and the ζ^{th} summand $\big(R_\zeta(g) \cdot Q_\zeta(g)\big)(K)$ is the ζ-eigenspace, proving diagonalizability.

For g of order exactly m, with $m|n$, let ζ be a primitive m^{th} root of unity, and $v \in K$ a ζ-eigenvector. Then v^m is fixed by G, so is in k, while v itself is fixed by no proper subgroup of G. By Galois theory $K = k(\sqrt[m]{v^m}) = k(\sqrt[n]{v^n})$... [cont'd]